

MAIN FACS Security Administration Monitoring Checklist

FACS Agency Code _____ Agency Name _____
Monitoring Period: _____ to _____

This list is a guide for agencies to highlight key security administration issues that should be monitored routinely (bi-weekly, monthly, or semi-annually depending on the monitoring technique and/or the number of user ids assigned to an agency) to ensure that good internal controls are in place. Please keep in mind agencies may have specific issues that need to be addressed and, therefore, this list should not be considered as all-inclusive. Canned MIDB scripts in the 'Security' script group have been identified to assist with your monitoring efforts as well as recommended intervals of time to monitor the security administration issues.

Overall Issues

1. Identify and review multiple user ids assigned to a user and determine if multiple user ids are still needed. If they are, verify that incompatibilities do not exist among the user ids assigned to a user.

MIDB Script: RACF 07 – Users With Multiple User IDs

Recommended Interval: Semi-annually

2. Identify user ids belonging to departed or retired employees and request that they be deleted. Determine if transactions have been processed with the user ids since the departure date.

MIDB Script: RACF 04 – User IDs That Belong To Departed Employees

Recommended Interval: Bi-weekly

3. Identify user ids belonging to employees on leave of absence or on workers compensation and revoke or delete their access until the users return to work. Determine if transactions have been processed with the user ids since the user has been on leave.

MIDB Script: RACF 05 – User IDs That Belong To Employees on LOA or Workers Comp

Recommended Interval: Bi-weekly

4. Identify user ids that haven't been used in the last 6 months (or less) and determine if access is still needed.

MIDB Script: RACF 03 –Users Not Using Their RACF IDs

Recommended Interval: Semi-annually

5. Identify user ids that belong to employees who have had a job change and determine if access is still appropriate for their new job function.

MIDB Script: RACF 06 –User IDs & Job Changes/Process Level Changes

Recommended Interval: Bi-weekly

6. Maintain files of deleted user ids and user names for future referencing to document authorization tracking screens.
MIDB Script: None
Recommended Interval: Always
7. Verify security requests are entered correctly in ADPICS and RSTARS by OFM.
MIDB Script: None
Recommended Interval: Periodically
8. Compare security request forms to the security framework to ensure compliance before sending to OFM.
MIDB Script: None
Recommended Interval: Always
9. Verify RACF password resets were performed by appropriate staff for legitimate requests from users.
MIDB Script: RACF 09 – Password Resets
Recommended Interval: Weekly

ADPICS Specific

1. Coordinate a review of all users' security privileges in ADPICS to determine if access is still appropriate for users' job functions (e.g., user classes, document/document types, user departments, mailbox departments, department authorizations).
MIDB Script: ADPICS 09 – ADPICS Security Assigned to User IDs
Recommended Interval: Quarterly
2. Compare users' security privileges to privileges documented in the security framework schedules and make applicable adjustments.
MIDB Script: None
Recommended Interval: Always
3. Verify that the use of wildcards (***) in the user department, mailbox department, and department authorization fields on users' security profiles is still applicable.
MIDB Scripts: ADPICS 10 – User IDs With Wildcards (*) Assigned To User Departments, ADPICS 11 – User IDs With Wildcards (*) Assigned To Mailboxes, and ADPICS 12 – User IDs With Wildcards (*) Assigned To Department Authorizations
Recommended Interval: Quarterly
4. Verify appropriate approval paths have been set up for each active ADPICS purchasing department and for every critical document/document type assigned to users.
MIDB Scripts: ADPICS 06 – ADPICS Doc/Doc Type With No Approval Path and ADPICS 07 – Initiating Department Approval Path
Recommended Interval: Semi-annually

5. Identify transactions in ADPICS that have been initiated and authorized by the same user id and verify propriety. Modify user security and/or approval paths to prevent this from occurring again or implement compensating internal controls to offset the risks involved with these types of situations.

MIDB Script: ADPICS 15 – Documents Initiated and Approved By Same User ID

Recommended Interval: Monthly

6. Identify ADPICS departments with no activity and determine if the departments should still be assigned to users' security and/or inactivated on the 5970 screen in ADPICS.

MIDB Script: ADPICS 13 – Purchasing Departments With No Activity

Recommended Interval: Semi-annually

7. Identify users with User Class 17 in ADPICS and verify that access is still needed. Obtain assurance that compensating internal controls are in place to address risks of assigning this user class.

MIDB Script: ADPICS 03 – ADPICS Users By Class

Recommended Interval: Quarterly

8. Verify that the accounts payable exception processing capability is restricted and exercised properly.

MIDB Script: ADPICS 14 – Users With Exception Processing Capabilities and/or PURCH 03 – Voucher Exception Report (from the Purchasing Script Group)

Recommended Interval: Monthly

RSTARS Specific

1. Coordinate a review of all users' security privileges to determine if access is still appropriate for users' job functions (e.g., user classes, agency ranges, bank codes).

MIDB Script: RSTARS 08 – Summary of RSTARS Security Assigned to User IDs

Recommended Interval: Semi-annually

2. Compare users' security privileges to the privileges documented in the security framework schedules and make applicable adjustments.

MIDB Script: None

Recommended Interval: Always

3. Identify and review users with incompatible user class assignments in RSTARS and verify that access is still needed. Obtain assurance that compensating controls are in place to address risks associated with incompatible assignments.

MIDB Script: RSTARS 04 – Security User Class Conflicts

Recommended Interval: Quarterly

4. Identify and review users with undesirable user class assignments in RSTARS and verify that access is still needed. Obtain assurance that compensating internal controls are in place to address risks of undesirable assignments.

MIDB Script: RSTARS 07 – Undesirable User Class Assignments

Recommended Interval: Semi-annually

5. Identify and review User Class 48/User Class 49 transactions for propriety and appropriate coding.

MIDB Script: RSTARS 14 – FY04 UC48/UC49 Transactions

Recommended Interval: Monthly

6. Review decentralized warrants printed with User Class 77 for propriety and frequency.

MIDB Script: RSTARS 20 – Locally Issued and Manually Written Warrants

Recommended Interval: Monthly